Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

The Information Commissioner's Office (ICO) response to the joint consultation from the Law Commission and Scottish Law Commission entitled 'Automated Vehicles: Consultation Paper 3 – a regulatory framework for automated vehicles'

About the ICO

1. The Information Commissioner has responsibility for promoting and enforcing the UK General Data Protection Regulation ('UK GDPR'), the Data Protection Act 2018 ('DPA'), the Freedom of Information Act 2000 ('FOIA'), the Environmental Information Regulations 2004 ('EIR'), the Privacy and Electronic Communications Regulations 2003 ('PECR') and the Network and Information Systems Regulations 2018 ('NIS').

2. The Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

Introduction

3. The ICO is pleased to respond to this joint consultation and notes the prior engagement on this topic. The ICO seeks to encourage public trust in how personal data is used to support innovation, economic growth and societal benefits. Whilst automated vehicle technology has the potential to deliver such benefits through improved road safety and user convenience, there is a need to consider the volume and nature of the data that vehicles may generate. Adopting appropriate safeguards will ensure transparency, fairness, accountability and user control whilst also preventing the misuse of individuals' personal data.

4. The ICO has previously provided guidance on automation in transport, contributing to the Global Privacy Assembly resolution on data protection in automated and connected vehicles and the International Working Group on Data Protection in Technology's working paper on connected vehicles. More recently we responded to the UK Government Centre for Connected and Autonomous Vehicles' call for evidence on Automated Lane Keeping Systems (ALKS).

5. This response focuses on those areas of the consultation that are within the ICO's remit, which are mainly contained in Chapter 17 and Appendix 4. We have provided some general observations but recommend referring to the pieces of guidance linked above for wider considerations.

Legislative landscape

6. Further consideration needs to be given to the general legislative landscape in the UK in which automated vehicles will operate. The consultation refers to Directive 2002/58/EC, known as the ePrivacy Directive ('ePD'), however reference should instead be made to PECR, which is the UK law that gives effect to the ePD.

7. Section 17.54 notes that the legislator "clearly did not have AVs [automated vehicles] in mind" when the Directive was enacted, and that "At the time, the typical terminal equipment was a telephone handset". It is important to note that both PECR and the ePD are intentionally technology neutral, and intend to provide specific rules for terminal equipment on the basis that it is part of the individual's 'private sphere' and requires protection from unwarranted intrusion. Therefore, care must be taken when interpreting the legislation, so that its underlying rationale, and technology neutral approach is fully understood and any proposals accord with its objectives. The ICO has produced guidance on PECR that provides further information.

8. Additionally, reference is made to the ePrivacy Regulation[1] that has been proposed by the European Commission but at present has yet to be negotiated with the European Parliament and formally published, so is not yet law. Whilst it will be important to consider such proposals and how they may impact the legislative landscape in respect of automated vehicles when they are further developed, sections 4.48-4.50 of Appendix 4 appear to be speculative and not directly relevant to the UK's legal regime.

9. The legislation referred to in the consultation also needs to be updated to reflect the UK's legal position now the transition period out of the European Union has ended. For example, there is currently no guarantee that the ePrivacy Regulation will be transposed into UK law and references to the GDPR should now be to the UK GDPR. There should also be reference to the Data Protection Act 2018, which does not appear to be mentioned in the consultation.

[1] Available at https://eur-lex.europa.eu/procedure/EN/2017_3

10. As such, the ICO strongly recommends that Chapter 17 and Appendix 4 are reviewed to account for the current legislative landscape in the UK. In general, further detail on what legislation applies in each circumstance outlined in the consultation would be beneficial, as this will depend upon various factors such as what the processing is, where it takes place and who it targets.

Personal data

11. Chapter 17 and Appendix 4 of this consultation acknowledge that much of the data that is generated by an automated vehicle will be personal data, as defined by Article 4(1) of the UK GDPR. Where information processed by an automated vehicle constitutes personal data, it must be processed in accordance with data protection legislation[2].

12. Automated vehicles pose particular challenges in relation to personal data, as often they will process the personal data of several individuals: owners, drivers, passengers and even pedestrians. If the personal data of these users is processed inappropriately, there is a heightened risk of intrusion into individuals' work and private lives. The Government and technology providers should therefore adopt a data protection by design and default approach, ensuring that privacy protections are built into the design and development of automated vehicles. The ICO has produced detailed guidance on determining what is personal data that provides further information.

13. Appendix 4 notes that additional protection is given to special category data under data protection legislation due to its sensitive nature. This is because use of this data could create significant risks to individuals' fundamental rights and freedoms, so its processing requires greater protection. Appendix 4 notes that in respect of processing special category data for insurance claims, controllers must satisfy a UK GDPR Article 9 condition in addition to identifying an Article 6 lawful basis. However, further clarity is welcomed on this section, as there appears to be confusion between satisfying a condition in Article 9(2) of the UK GDPR and the requirements of section 10 of the DPA 2018.

14. Section 17.48 considers that location data has the potential to reveal further information about an individual, such as information pertaining to an individual's sex life through visits to a particular location. It is important to distinguish here between an inference and a factual record. Care needs to be

[2] For ease of reference, data protection legislation is used to refer to the UKGDPR and the DPA 2018.

taken to ensure that inferences about an individual can be made with certainty to consider it special category data. Assuming someone's sex life through multiple visits to a specific location is tenuous and could lead to inaccurate personal data. More information on inferences and educated guesses can be found in the ICO's guidance on special category data.

Anonymisation

15. Chapter 17 outlines that datasets will be anonymised. Explanation is required that details what anonymisation techniques will be used and how they will render personal data truly anonymous. If data is truly anonymous, then it will not be personal data as defined by the UK GDPR and thus will not be subject to data protection legislation.

16. However, in determining this, consideration needs to be given to whether, via means reasonably likely to be used, individuals are identifiable as this would only constitute pseudonymisation, not anonymisation and would thus still be in scope of data protection legislation. True anonymisation is difficult to achieve and there needs to be a thorough and documented risk assessment of the risk of reidentification. If the information remains in scope of data protection legislation, it must be processed in compliance with its requirements, with appropriate technical and organisations measures and safeguards in place.

Transparency

17. The requirement to provide privacy information to individuals in relation to how their personal data will be processed is a fundamental right under the data protection legislation. Individuals have the right to be informed about the collection and use of their personal data and they must be provided with such information at the time when their personal data is collected.[3] Further, data should not be processed in a way which data subjects would not reasonably expect.

18. The provision of privacy information is particularly of importance in relation to automated vehicles as the data subjects may not be limited to the owner of the vehicle, but include other drivers and passengers as well as those whom are observed through sensor technology on the vehicle, such as pedestrians.

[3] If an individual's personal data is obtained indirectly eg from a source other than the individual, the timeframe for providing transparency information is set out in Article 14 of the UK GDPR.

19. The limited, and sometimes non-existent, physical interfaces on automated vehicles pose challenges when trying to inform data subjects about the use of their personal data. In cases where controllers may not be able to display privacy information in an obvious way (for example as part of a website or via providing the information to all data subjects upon purchase or use of an automated vehicle), they need to consider alternative methods. Careful consideration should be taken regarding what format is the most appropriate under the circumstances. Privacy information must also be regularly reviewed to ensure that any new use of an individual's personal data is brought to that individual's attention before the processing begins.

20. In respect of rental vehicles and car owners, any personal data that must be retained after ownership of a car has ended should have a clear purpose with a defined retention periods appropriate for that purpose, and owners should be made aware of this. This should not be accessible to any future users of the vehicle. Further guidance on providing data subjects with privacy information can be found here.

Data subjects' rights

21. The UK GDPR provides individuals with a number of rights in respect of their personal data. These are outlined in Articles 15 – 22 and include the rights to be informed about how personal data is being processed, the right of subject access, the right to get inaccurate data rectified, the right to restrict processing and the right to object to processing. Appendix 4 notes at 4.18 that some of these rights may be relevant to that data processed in relation to an automated vehicle. The ICO would suggest clarification is given here to explain that all processing of personal data in the context of automated vehicles will be subject to data protection legislation, including application of data subject rights across Articles 15 to 22, subject to the provisions of the law.

22. Automated vehicles pose a risk to individual's rights, if they have insufficient control over their data in order to assert their data protection rights. Therefore, care must be taken by controllers in the automated vehicle ecosystem to ensure that such risks are adequately mitigated and addressed. The ICO's guidance on individuals rights provides further information that should be referred to.

Data minimisation

23. Appendix 4 notes at 4.16 that there is a "strong emphasis" in the UK GDPR "on discarding unnecessary data". However, data protection legislation requires controllers to only process personal data that is adequate, relevant and limited to what is necessary in relation to their purpose. This puts the onus on controllers to only collect data which is necessary in the first place, rather than collecting unnecessary data and then discarding it.

24. In deciding whether the amount of data they process is limited to what is necessary, controllers must be clear about why they need the data. This is particularly important when the data is special category data or criminal offence data. The ICO has produced guidance on data minimisation and purpose limitation that provides further detail on this requirement.

Recording of location data

25. Throughout the consultation, proposals outline the need for data to be processed in various ways, such as through event data recorders, collecting near miss data and recording the location and time at which the Automated Driving System is activated and deactivated. The UK's data protection legislation requires that processing is necessary, proportionate and limited to no more than what is needed to achieve the purpose. Therefore, any proposals relating to the establishment of a national system to process this data will need to clearly demonstrate why this is necessary, how it is proportionate and how it will meet data protection requirements. Further evidence and rationale is required to support such an assertion, with necessity and proportionality tests undertaken.

26. Location data in this context needs to be defined further. For example, whilst the UK GDPR references location data in the context of the definition of personal data, PECR has a specific definition for its purposes. Any processing of location data that meets this definition will need to comply with the relevant provisions of PECR in this regard.

27. Appendix 4 outlines the Law Commission view that the scheme proposed for automated vehicles is a public security measure for the purposes of the ePD. As outlined in the legislative landscape section above, reference needs to be made to the relevant UK law, PECR, not the EU ePD upon which PECR is based. Article 15 of the ePD is not an exemption that can be relied on in its own right. The purpose of Article 15 of the ePD is to allow for restrictions (ie

exemptions) on the obligations and rights provided within the Directive, where such a restriction is a necessary and proportionate measure to achieve particular objectives, such as 'public security'. The relevant restrictions in PECR currently relate to 'national security' and 'law and crime', found in Regulations 28 and 29 respectively, and only apply to communications providers.

28. Aside from these general exemptions that can apply to any of the PECR rules, some PECR rules have built-in exemptions. Organisations ultimately need to consider whether any PECR exemptions apply in the given circumstances.

29. In the context of connected vehicles, organisations should be particularly mindful of PECR Regulations 6 and 14.

30. Regulation 6 contains a general prohibition on the storage of information, or access to information stored, in the terminal equipment of the subscriber or user without the provision of clear and comprehensive information about the purposes of such storage or access, and prior consent (which must be to the UK GDPR standard). Regulation 6 does however contain exemptions to this requirement and the ICO's guidance provides further detail.

31. Regulation 14 places strict rules on the processing of location data and does not contain any built in exemptions. As outlined in ICO guidance, there are two exemptions to Regulation 14 – Regulation 16 and 16A – which are emergency calls and emergency alerts, so these would likely not be relevant to the proposals contained in this consultation.

Disclosing personal data to insurers

32. Section 17.67 of the consultation appears to suggest that the UK GDPR Article 6(1)(c) lawful basis of legal obligation is "simpler" to use in order to disclose personal data to insurers rather than being the most appropriate in the circumstances. The ICO strongly suggests that the relevant consideration is not whether a particular lawful basis is the simplest to use but whether it is the most appropriate in the context of the overall processing activity.

33. The consultation notes that this duty to disclose to insurers could be imposed on "those controlling" the automated vehicle data, however it is unclear if this would be the manufacturer, the driver, the vehicle owner or another party. Clarity on whom this duty is proposed to be imposed on is

needed. Given the importance of the data protection legislation's accountability principle, the roles and responsibilities of controllers, joint controllers and processors must be decided at the outset. The ICO has created guidance on controllers and processors that may be of use in determining the controller of the personal data. Additionally, the ICO has developed an Accountability Framework that may assist responsible parties in determining how to comply with their obligations.

34. This proposal suggests that the duty to disclose data to insurers will only apply where the data is necessary to decide claims. Therefore, it is important for controllers to ascertain what is necessary.

35. It appears that the proposals outlined in this section may be possible with data being recorded on the connected vehicle and being accessible through existing legal gateways. Further clarification is therefore needed to explain why the requirement for data in this instance is different from that at present where in all motor accidents, the insurer needs to establish if a claim is genuine. The consultation suggests that the only difference from the present circumstances is that in relation to strict liability, if causation is proven then there will be no need to prove negligence. It is unclear how there is any difference in respect of automated vehicles which would mean precise location data is always required and thus that legislation should impose a duty requiring collection and disclosure.

36. In any event, sharing of personal data with insurers in the context of automated vehicles should be limited and proportionate, with appropriate safeguards such as access to the data and limits on the type and volume of data. The data protection legislation does not prevent appropriate and proportionate data sharing in the public interest, including when it is necessary to protect the public, for insurance purposes, or in an emergency – it provides a framework in which data sharing can be undertaken in a fair and proportionate way. The ICO's Data Sharing Code of Practice as well as other guidance referenced throughout this response will assist organisations processing personal data in the context of automated vehicles in this regard.

37. Additionally, any sharing of personal data for law enforcement purposes will be subject to Part 3 of the DPA and require those bodies processing the personal data to be competent authorities, as defined in section 30 of the DPA. These competent authorities will need to be clear about their responsibilities, such as the need to consider undertaking a DPIA under s64 of

the DPA. The ICO has produced guidance on law enforcement processing under the DPA which may be of use here.

Retention of data

38. Article 5(1)(e) of the UKGDPR notes that personal data should be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed". This is known as the storage limitation principle. Additionally, to comply with documentation requirements in the UK GDPR, controllers should have a policy setting out standard retention periods wherever possible. Furthermore, in line with a data protection by design and default approach, appropriate technical measures should be put in place to give effect to any such organisational policies in a way that ensures effective implementation of the principle.

39. Where the data referred to in sections 17.72–17.80 is personal data, the retention period is a matter for the controller of that data, unless the Law Commission is suggesting a standard retention period, such as through legislation, industry standards, or codes of conduct. Further clarity on this is welcomed in line with the accountability requirements set out in the next section of this response.

40. It is important that controllers are able to justify and explain why personal data is needed for the length of time chosen and that this period is not longer than is necessary. Further, any retention period should be periodically reviewed to ensure that it is appropriate, especially if the standard retention period is lengthy or there is potential for a significant impact on individuals.

41. Care should be taken not to impose blanket retention periods for all types of data, as some 'Data Storage Systems for Automated Driving' data may be needed for longer than others depending on the purpose for which those types of data are processed. For example, whilst some data may need to be kept to comply with a legal obligation, it is unlikely that other information gathered in vehicles (that may not be strictly linked to being an automated vehicle) needs to be kept, such as a consumer's music history or contacts if these have been processed. The ICO has produced guidance that provides further information on storage limitation that should be referred to in developing and reviewing the retention period.

42. It is worth noting that reference is made within the consultation to data being anonymous. If the data is truly anonymous, bearing in mind the

considerations already outlined earlier in this response, then it is outside the scope of data protection legislation and the data minimisation principle.

Accountability

43. The ICO supports the view that systems should only be allowed to operate if they are in compliance with data protection legislation, noting that in the UK this is the UK GDPR and the DPA 2018. Additionally, we suggest that the regulator referred to should only categorise a system as self-driving if it is satisfied that the automated driving system entity (ADSE) has systems to abide by its obligations under the PECR.

Data protection by design and default

44. Article 25 of the UK GDPR requires controllers to adopt a data protection by design and default approach. This means they need to have appropriate technical and organisational measures in place that implement the data protection principles effectively and safeguard individual rights. These need to be in place from the design stage, so all controllers involved in the automated vehicle lifecycle must abide by this requirement. The monitoring of individuals through an automated vehicle has the potential to be particularly intrusive so again, the ICO highlights the importance of adopting a data protection by design and default approach to ensure the minimal amount of data is processed.

Data protection impact assessment (DPIA)

45. Data controllers are required to undertake a DPIA in certain circumstances, as outlined in Article 35 of the UK GDPR. A DPIA allows controllers to identify and minimise any data protection risks. DPIAs are required by law to be carried out where processing is likely to result in a high risk for individuals. The ICO has a list of processing activities where a DPIA must be undertaken in addition to the Article 35(4) list in the UK GDPR.

46. It is likely that a range of controllers will need to undertake DPIAs in respect of connected and autonomous vehicles. For example, this may include manufacturers, suppliers and those in control of the ADSE, so as to adequately identity and mitigate any risks associated with the ADSE under Article 35 of the UK GDPR and detail which party is responsible for what aspects of any personal data processing. A DPIA should outline, amongst other things, how personal data will be recorded, stored, accessed and

protected. If controllers are not able to sufficiently mitigate a high risk posed to data subjects in relation to the ADSE within their DPIA, they must consult with the ICO under Article 36(1) of the UK GDPR prior to processing the data.
Codes of Conduct

47. Section 17.92 of the consultation suggests that in time, good practice can be included in an industry code of practice. The Law Commission may wish to consider whether, in its recommendations, it calls for an industry Code of Conduct under the UK GDPR as this may be a more effective way of ensuring a level of compliance industry wide. Under Article 40 of the UK GDPR only a trade body or association can prepare such a code. The regulator could then also give consideration as to whether the ADSE complies with the Code of Conduct. More information on Codes of Conduct under the UK GDPR can be found here.

Legislative consultation

48. In respect of the proposal for the Government to work within the UNECE to ensure data storage systems for automated driving record data, it is again important to make such considerations within the context of the UK legislative landscape. If the UK decides to apply the UNECE, it will need to amend the Road Vehicles (Approval) Regulations 2020 to incorporate the provisions on the UN regulation into domestic law. This will require amendments to Schedules 1 and 2 relating to the technical and administrative requirements. Any decision to do this is a matter for Government. If the Government plans to do this, it will need to consult the ICO under Article 36(4) of the UK GDPR.

49. Article 36(4) requires Government to formally consult the ICO during the preparation of policy proposals for legislative or statutory measures relating to the processing of personal data. Guidance on the application of Article 36(4) can be found here.

50. This will also be relevant if Government develop legislation to impose a duty on those controlling automated vehicle data to disclose said data to insurers, or to work within the UNECE to ensure data storage systems retain particular data.

Conclusion

51. We hope the above comments are of use in developing any proposals relating to automated vehicles further. The ICO would welcome engagement

with the Scottish and UK Governments, the Department for Transport and CCAV to help ensure the issues identified are adequately addressed.

The Information Commissioner's Office

March 2021